(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 61 102 A 1**

(51) Int. Cl.[7]: G 06 F 17/30

(21) Aktenzeichen: 100 61 102.8
(22) Anmeldetag: 7. 12. 2000
(43) Offenlegungstag: 27. 6. 2002

DE 100 61 102 A 1

(71) Anmelder:
TC TrustCenter AG, 20097 Hamburg, DE

(74) Vertreter:
Eisenführ, Speiser & Partner, 28195 Bremen

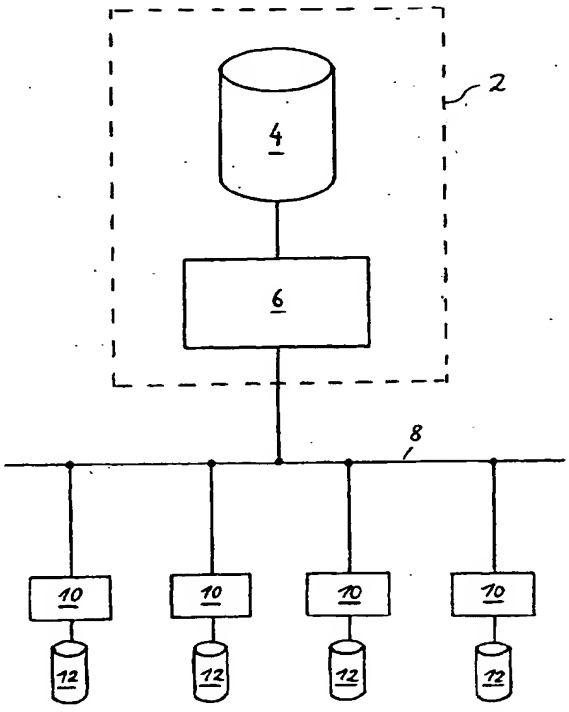
(72) Erfinder:
Hiller, Stephan, 22081 Hamburg, DE; Lindemann, Rolf, Dr., 21224 Rosengarten, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) System zur Statusabfrage von digitalen Zertifikaten

(57) Die Erfindung betrifft ein System zur Stauabfrage von digitalen Zertifikaten mit einer zentralen Zertifikatstatusdatenbank (4). Das Besondere der Erfindung besteht darin, daß eine Vielzahl von lokalen Zertifikatstatusdatenbanken (12), die von außen zugänglich sind und als Datenbestand jeweils nur eine Teilmenge des Datenbestandes der zentralen Zertifikatstatusbank (4) enthalten, und eine Repliziereinheit (6, 8, 10) zum Abgleich des Datenbestandes der lokalen Zertifikatstatusdatenbanken (12) jeweils mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (4) vorgesehen sind.



DE 100 61 102 A 1

Beschreibung

[0001] Die Erfindung betrifft ein System zur Statusabfrage von digitalen Zertifikaten, mit einer zentralen Zertifikatstatusdatenbank.

[0002] Aufgrund der weltweit steigenden Teilnehmerzahlen in elektronische Netzen und insbesondere im Internet ist auch eine Zunahme von Waren und Dienstleistungen, die über derartige elektronische Netze angeboten werden, zu beobachten. Der Handel mit Waren und das Anbieten von Dienstleistungen über elektronische Netze und insbesondere über das Internet wird im allgemeinen auch als e-Commerce bezeichnet.

[0003] Während es häufig vom Vorteil ist, sich in elektronischen Netzen anonym zu bewegen, um keine Datenspur zu hinterlassen, verlangt gleichwohl ein Großteil der Möglichkeiten, die bereits jetzt und auch in Zukunft elektronische Netze bieten, bestimmte Voraussetzungen in bezug auf die Nachprüfbarkeit der Identität einer Person. Dies ist besonders wichtig bei der Übertragung von vertraulichen Daten, insbesondere wenn die Person Zugriff auf fremde Daten haben kann. Dies gilt unter anderem auch für den Bereich des e-Commerce.

[0004] Zu den Voraussetzungen zählt die Gewährleistung von Sicherheit, Authentizität und Integrität übertragener Informationen.

[0005] Die Forderung nach Sicherheit der elektronischen Kommunikation als erste der zuvor genannten Voraussetzungen folgt aus dem schlichten Umstand, daß es nur mit geringem Aufwand möglich ist, die Kommunikation und somit den Datenaustausch zwischen zwei oder mehreren Parteien abzuhören. Ein Ausweg besteht nun darin, die Kommunikation zu verschlüsseln und somit für Dritte unlesbar zu machen.

[0006] Mit Hilfe der Authentizität als zweite der zuvor genannten Voraussetzungen ist es ferner möglich, Willensäußerungen einer bestimmten Person zuzuordnen. Durch die Authentizität ist es für die eine Person möglich, sich gegenüber einer anderen Person auszuweisen oder dieser gegenüber nachzuweisen, daß eine bestimmte Tätigkeit bzw. ein bestimmtes Dokument von dieser einer Person durchgeführt bzw. erstellt wurde. Authentizität wird durch eine digitale Signatur hergestellt.

[0007] Durch die Integrität als dritte der zuvor genannten Voraussetzungen wird sichergestellt, daß Information, Daten und Dokumente nicht durch Dritte unbefugt geändert werden können, ohne daß dies bemerkbar wäre. Die Integrität wird durch einen sogenannten Hashwert gewährleistet, der der digitalen Signatur zugrunde liegt.

[0008] Alle drei genannten Voraussetzungen können durch die Nutzung der Public-Key-Kryptographie realisiert werden. Hierbei besitzt jeder Nutzer ein sogenanntes Schlüsselpaar, welches sich aus einem sogenannten Private Key und einem sogenannten Public Key zusammensetzt. Während der Private Key im allgemeinen gut geschützt ist, beispielsweise durch Verschlüsselung auf einem Datenträger wie z. B. einer Chipkarte, wird der Public Key dem Kommunikationspartner für Verschlüsselungszwecke zur Verfügung gestellt. Beide Schlüssel sind komplementär zueinander; d. h. was der eine verschlüsselt, kann nur von dem anderen wieder entschlüsselt werden. Zum Zwecke der Informationsverschlüsselung wird aber nur der Public Key des Empfängers verwendet, während mit dem Private-Key, den nur der rechtmäßige Besitzer hat, die an ihn gerichtete verschlüsselte Nachricht wieder in lesbare Form gebracht werden kann.

[0009] Neben der Entschlüsselung wird der Private Key auch noch zur Signaturbildung benutzt, um die Forderung nach Authentizität und Integrität zu realisieren. Bei der Signaturbildung wird zunächst der bereits zuvor erwähnte Hashwert über die zu signierenden Daten berechnet. Auf diese Weise wird die Integrität gewährleistet, da eine Änderung in den signierten Daten auch zwangsläufig zu einer Änderung des Hashwertes führt. Dieser Hashwert wiederum wird mit Hilfe des Private Key des Verfassers bzw. Absenders verschlüsselt. Auf diese Weise wird die Authentizität gewährleistet, da lediglich der rechtmäßige Besitzer über den Private Key verfügt.

[0010] Allerdings ist mit der reinen Existenz eines Private Key und eines Public Key noch nicht festzustellen, wem der Public Key, der für Verschlüsselungszwecke bereitgestellt wird, gehört. Um hier eine eindeutige Zuordnung zwischen dem Schlüsselpaar und der berechtigten Person vorzunehmen, haben sich vertrauenswürdige Instanzen etabliert, die als Zertifizierungsstellen bezeichnet werden und als Dienstleistung die Identifizierung von Personen und die anschließende Ausstellung eines sogenannten digitalen Zertifikates anbieten.

[0011] Ein digitales Zertifikat besteht aus Informationen über den Zertifikatsinhaber (z. B. Name, Ort, Land, Firma, Abteilung, Adresse etc.), den Namen des Zertifikatsausstellers, den Gültigkeitszeitraum und den Public Key sowie aus der Signatur der Zertifizierungsinstanz.

[0012] Durch die Signatur der Zertifizierungsinstanz wird die Unverfälschbarkeit der im Zertifikat enthaltenen Angaben gewährleistet. Dies ist aber nur dann sinnvoll, wenn der Zertifizierungsinstanz ein entsprechendes Vertrauen bei der Ausstellung und dem Management vom Zertifikaten entgegengebracht wird.

[0013] Bei der Zertifizierungsinstanz ist die eingangs erwähnte zentrale Zertifikatstatusdatenbank eingerichtet, in welcher der Status von sämtlichen von der Zertifizierungsinstanz verwalteten Zertifikaten abgespeichert ist.

[0014] Während der Gültigkeit des Zertifikates gemäß Gültigkeitszeitraum kann nun eine dritte Person, z. B. ein Anbieter von Waren und/oder Dienstleistungen, davon ausgehen, daß die Angaben im Zertifikat, welches ihm vom Zertifikatsbesitzer vorgelegt wird, der Wahrheit entsprechen, wenn sie das Zertifikat verifiziert hat.

[0015] Allerdings kann es vorkommen, daß ein Zertifikatsbesitzer seinen Datenträger (z. B. Chipkarte) mit dem Private Key verliert oder das der Private Key von einem Dritten kopiert und somit kompromittiert wurde. Um in einem solchen unerwünschten Fall den Mißbrauch so gering wie möglich zu halten, kann der Besitzer sein Zertifikat bei der Zertifizierungsinstanz, von der es auch ausgestellt wurde, umgehend sperren (revozieren) lassen.

[0016] Die Zertifizierungsinstanz trägt in ihrer zentralen Zertifikatstatusdatenbank einen Verweis auf das betreffende Zertifikat in eine sogenannte Sperrliste (Certificate Revocation List, abgekürzt CRL) ein, die für jeden öffentlich zur Verfügung gestellt wird und dabei als Grundlage für eine Überprüfung von Zertifikaten dient. Bei einer solchen Sperrliste handelt es sich demnach um eine Negativliste, die nicht den gesamten Datenbestand, sondern lediglich die gesperrten Zertifikate, in der Regel deren Seriennummern, angibt.

[0017] Obwohl die Sperrliste lediglich die gesperrten bzw. revozierten Zertifikate angibt, kann ihre Größe zu einem Problem werden. So muß bei jeder Überprüfung die aktuelle (relevante) Sperrliste vorliegen. Da Sperrungen jederzeit auftreten, muß auch die Sperrliste zu jedem Zeitpunkt entsprechend neu erstellt werden. Um ständig die aktuellen Sperrinformationen verfügbar zu haben, muß die Sperrliste bei jeder Überprüfung neu abgefragt werden. Da die Sperrliste den gesamten Datenbestand sämtlicher von der Zertifi-

zierungsstelle gesperrten Zertifikate beinhaltet, wird für ihre Übertragung eine große Bandbreite benötigt.

[0018] Ein weiterer Nachteil der Sperrliste besteht darin, daß eine darauf basierende Aussage nur dann eine Positivaussage ist, wenn das entsprechende Zertifikat tatsächlich in der Sperrliste angegeben und somit gesperrt ist. Ansonsten läßt die Sperrliste hinsichtlich der gültigen Zertifikate nur eine Negativaussage zu, indem der Umkehrschluß dergestalt gezogen werden muß, daß das Nichtvorhandensein eines Zertifikates in der Sperrliste auf dessen Gültigkeit schließen läßt. Demnach ist aber bei Verwendung einer solchen Sperrliste eine Kompromittierung des Private Key der Zertifizierungsstelle oder eine unberechtigte Ausstellung eines Zertifikates nicht ohne weiteres erkennbar, da in einem solchen Fall das Zertifikat zumindest zunächst eine als gültig anerkannte Signatur der Zertifizierungsstelle besitzt, und zwar so lange, bis dieses Problem erkannt und aufgrund dessen das Zertifikat gesperrt wird.

[0019] Eine Alternative zum Anlegen einer Sperrliste besteht in der Bereitstellung eines Online-Zertifikatstatusprotokoll-Dienstes durch die Zertifizierungsstelle. Dieser Dienst wird auch als Online-Certificate-Status-Protocol-Dienst oder, abgekürzt, als OCSP-Dienst bezeichnet. Mit diesem Dienst wird ein Protokoll zur Verfügung gestellt, mit dem gezielt der Status einzelner Zertifikate und überlicherweise nur eines einzelnen Zertifikates überprüft werden kann. Hierdurch ist es möglich, die von vielen Anwendungen geforderte Aktualität zu gewährleisten. Allerdings stößt auch dieser Dienst bei einer hohen Anzahl zu überprüfender Zertifikate schnell an die Grenzen seiner Leistungsfähigkeit. Dadurch ist dieser Dienst im Hochlastbereich nur bedingt einsatzfähig, zumal durch die große Anzahl von Abfragen auch hier eine entsprechende Bandbreite notwendig ist, um die Antworten mit hoher Aktualität zu versenden.

[0020] Die beiden zuvor beschriebenen Verifikationsverfahren decken zwei konträre Extremfälle ab. Die Sperrliste eignet sich für die Verifikation einer hohen Anzahl von Zertifikaten, da der komplette Datenbestand der gesperrten Zertifikate vorliegt. Allerdings führt hier die hohe Bandbreitenbelastung bei der Übertragung des Sperrlisteninhaltes und die daraus resultierende geringere Download-Wiederholfrequenz häufig zu einer mangelnden Aktualität.

[0021] Der Online-Zertifikatstatusprotokoll-Dienst hingegen zeichnet sich durch seine hohe Aktualität der Statusinformationen aus. Allerdings hat dieses Verfahren seine Grenzen dort, wo eine hohe Anzahl von Verifikationen pro Zeiteinheit durchgeführt werden müssen. Dies gilt sowohl für die Requestorseite (Anwender), wo die Anfrage generiert werden muß, als auch für die Responderseite (Zertifizierungsstelle), wo die Anfrage entgegengenommen und anschließend mit einer entsprechenden Antwort beantwortet werden muß. Zieht man weiterhin mehrere Requestoren pro Zertifizierungsstelle in Betracht, so kann sich leicht ein Volumen von mehreren hundert bis tausend Abfragen pro Sekunde ergeben.

[0022] Es ist nun Aufgabe der Erfindung, die vorteilhaften Eigenschaften der beiden zuvor erläuterten Verifikationsverfahren miteinander zu verknüpfen, ohne ihre Nachteile zu übernehmen.

[0023] Diese Aufgabe wird bei einem System der Eingangs genannten Art dadurch gelöst, daß eine Vielzahl von lokalen Zertifikatstatusdatenbanken geschaffen wird, die von außen zugänglich sind und als Datenbestand jeweils nur eine Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank enthalten, und eine Replizierеinrichtung zum Abgleich des Datenbestandes der lokalen Zertifikatstatusdatenbanken jeweils mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank vorgesehen ist.

[0024] Mit Hilfe der Erfindung wird also ein Konzept geschaffen, welches, ausgehend von einer zentralen Datenbank bei einer Zertifizierungsstelle, diverse lokal installierte Datenbanken aktualisiert. Diese lokalen Zertifikatstatusdatenbanken sind bei Kunden der Zertifizierungsstelle eingerichtet, bei welchen es sich gewöhnlich um Geschäfte, Banken oder sonstige Unternehmen handelt. Mit Hilfe eines Protokolls werden somit, ausgehend von der zentralen Zertifikatstatusdatenbank bei der Zertifizierungsstelle, die für einzelne Kunden relevanten Zertifikatstatusinformationen mit den jeweiligen lokalen Datenbanken abgeglichen. In den lokalen Datenbanken wird jedoch nicht der komplette Datenbestand der zentralen Zertifikatstatusdatenbank, sondern erfindungsgemäß nur der für den jeweiligen Kunden relevante Teil repliziert. Die Änderung eines Zertifikatstatus oder im Falle einer Neuausstellung eines Zertifikates die Einrichtung des zugehörigen Zertifikatstatus wird initial in der zentralen Zertifikatstatusdatenbank durchgeführt. Anschließend wird diese Änderung in die lokale Zertifikatstatusdatenbank des diese Änderung betreffenden Kunden übertragen.

[0025] Durch die erfindungsgemäße Einrichtung vieler verteilter lokaler Zertifikatstatusdatenbanken kann bei der Zertifikatsüberprüfung ein großes Abfragevolumen realisiert werden. Dadurch läßt sich für die Zertifikatstatusinformationen eine hohe Aktualität erzielen, so daß man für sämtliche Zertifikatstatusinformationen Aussagen erhält, die im wesentlichen den Charakter von Positivaussagen besitzen.

[0026] Zugriff auf die zentrale Zertifikatstatusdatenbank hat nur die sie verwaltende Zertifizierungsstelle; ein Zugriff von außen, also durch andere Personen wie beispielsweise Kunden ist erfindungsgemäß nicht möglich. Für den Anwender bzw. Kunden zugänglich ist erfindungsgemäß nur die ihm zugeordnete lokale Zertifikatstatusdatenbank, auf die selbstverständlich auch die Zertifizierungsstelle noch zugreifen kann.

[0027] Wegen der unterschiedlichen Kundenapplikationen sind die Datenbestände der lokalen Zertifikatstatusdatenbanken selbstverständlich unterschiedlich. Dabei handelt es sich erfindungsgemäß beim Datenbestand jeder lokalen Zertifikatstatusdatenbank jeweils um eine Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank, und zwar gewöhnlich derart, daß die Summe der Datenbestände aller lokaler Zertifikatstatusdatenbanken dem gesamten Datenbestand der zentralen Zertifikatstatusdatenbank entspricht.

[0028] Aufgrund der erfindungsgemäßen selektiven Datenübertragung an die dezentralen lokalen Datenbanken ist nur eine verhältnismäßig geringe Bandbreite erforderlich. Ein wesentlicher Vorteil der Erfindung in diesem Zusammenhang basiert auf der Annahme, daß die Abfragen eines Zertifikatstatus wesentlich häufiger vorkommen als die Änderung oder Neuausstellung von Zertifikaten. Die benötigte Bandbreite für die Nutzung eines Verifikationsdienstes kann somit drastisch gesenkt werden, da lediglich der Status der lokalen Datenbank und nicht jedes einzelne Zertifikat in der zentralen Zertifikatstatusdatenbank überprüft wird. Auf diese Weise läßt sich ein nahezu beliebiges Verifikationsvolumen bei relativ geringer Bandbreite realisieren.

[0029] Außerdem lassen sich mit Hilfe des erfindungsgemäßen Systems Zertifikate erkennen, die mit einem kompromittierten Zertifizierungsstellenschlüssel erstellt worden sind, da derartige Zertifikate zwar eine gültig scheinende Zertifizierungsstellensignatur besitzen, aber nicht in die zentrale Datenbank der Zertifizierungsstelle eingetragen worden sind. Dies hat zur Folge, daß auch solche gültig schei-

nenden, tatsächlich jedoch gefälschten Zertifikate bei einem Update unberücksichtigt bleiben und daher auch nicht von der Kundenapplikation als gültig betrachtet werden.

[0030] Schließlich besitzt das erfindungsgemäße System noch den Vorteil der Skalierbarkeit an die Bedürfnisse des jeweiligen Kunden.

[0031] Die Replizierereinrichtung sollte den Datenbestand mindestens einer lokalen Zertifikatstatusdatenbank in bestimmten, vorzugsweise gleichmäßigen, Zeitintervallen mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank wiederholt vergleichen.

[0032] Zweckmäßigerweise überprüft die Replizierereinrichtung, vorzugsweise regelmäßig, den Datenbestand der zentralen Zertifikatstatusdatenbank auf Änderungen und aktualisiert nur dann den Datenbestand einer lokalen Zertifikatstatusdatenbank, wenn sie in der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank Änderungen feststellt. Mit dieser Ausführung läßt sich eine besonders hohe Aktualität der Zertifikatstatusinformationen erzielen, während nur eine verhältnismäßig geringe Bandbreite bei der Übertragung benötigt wird, da nur bei Bedarf eine Aktualisierung der lokalen Zertifikatstatusdatenbanken vorgenommen wird.

[0033] Gewöhnlich weist die Replizierereinrichtung einen Server und ein Netzwerk auf, über das die lokalen Zertifikatstatusdatenbanken mit der zentralen Zertifikatstatusdatenbank verbunden sind. Die Replizierereinrichtung kann auch Teil eines vorhandenen Netzwerkes mit Server sein oder auch im Server eines Netzwerkes enthalten sein. Der Server steuert das Netzwerk und befindet sich überlicherweise bei der Zertifizierungsstelle. Dabei überträgt das Netzwerk Änderungen einer Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank an die zugehörige lokale Zertifikatstatusdatenbank. Alternativ kann die Replizierereinrichtung aber auch beispielsweise in der zentralen Zertifikatstatusdatenbank enthalten sein; es ist aber auch denkbar, die Replizierereinrichtung verteilt in den lokalen Zertifikatstatusdatenbanken vorzusehen.

[0034] Eine weitere gegenwärtig besonders bevorzugte Ausführung der Erfindung zeichnet sich dadurch aus, daß die Replizierereinrichtung von der zentralen Zertifikatstatusdatenbank zu den lokalen Zertifikatstatusdatenbanken Update-Nachrichten übermittelt, die mit einer Sequenznummer versehen sind und Zertifikationsinformationen, wie z. B. Seriennummer, Fingerprint, Zertifikatstatus und/oder Datum des aktuellen Status, enthalten.

[0035] Üblicherweise werden hierzu Protokolle übermittelt, die bestimmte Protokollelemente enthalten, von denen ein Protokollelement aus der zuvor erwähnten Update-Nachricht besteht.

[0036] Bei einer Weiterbildung der zuvor erwähnten Ausführung der Erfindung fragt die Replizierereinrichtung in der betreffenden lokalen Zertifikatstatusdatenbank die Sequenznummer der zuletzt empfangenen Update-Nachricht ab und vergleicht diese mit der Sequenznummer der zuletzt an diese lokale Zertifikatstatusdatenbank übertragenen Update-Nachricht in der zentralen Zertifikatstatusdatenbank und übermittelt nur im Falle einer Übereinstimmung eine nächste Update-Nachricht von der zentralen Zertifikatstatusdatenbank an die betreffende lokale Zertifikatstatusdatenbank. Auf diese Weise läßt sich die Aktualität der betreffenden lokalen Zertifikatstatusdatenbank verifizieren. Für diese Maßnahme bietet sich insbesondere die Verwendung eines Ping-Request und einer zugehörigen Ping-Response an. Um nämlich den Empfang einer Update-Nachricht zu bestätigen, wird vom Kunden bzw. von dessen lokaler Zertifikatstatusdatenbank ein Ping-Request mit der Sequenznummer der zuletzt empfangenen Update-Nachricht an den Server der Zertifizierungsstelle verschickt. Auf diesen Ping-Request antwortet der Server der Zertifizierungsstelle mit einer Ping-Response, die die Sequenznummer der zuletzt übertragenen Update-Nachricht enthält und somit die Aktualität der lokalen Zertifikatstatusdatenbank des Kunden bestätigt.

[0037] Weiterhin kann der zuvor erwähnte Ping-Request dazu dienen, sogenannte "Denial-of-Service"-Attacken zu erkennen, wenn die entsprechende Ping-Response oder Update-Nachricht nicht innerhalb eines vorbestimmten Zeitintervalls bzw. Timeouts zugestellt werden kann.

[0038] Das aus Ping-Request und Ping-Response bestehende Protokollpaar stellen die am häufigsten genutzten Protokollelemente dar, da üblicherweise die Bestätigung der Aktualität einer Datenbank wesentlich häufiger überprüft wird, als sich Änderungen oder Neuausstellungen von Zertifikaten ergeben.

[0039] Ferner kann eine Verifizierungseinrichtung zur, vorzugsweise regelmäßigen, Überprüfung der Integrität der Datenbestände der lokalen Zertifikatstatusdatenbänke vorgesehen sein, um eine (lokale) Manipulation zu erkennen und ggf. den Neuaufbau der betreffenden Datenbank zu veranlassen.

[0040] Üblicherweise vergleicht die Verifizierungseinrichtung die Datenbestände der lokalen Zertifikatstatusdatenbänke mit dem Datenbestand der zentralen Zertifikatstatusdatenbank. Ähnlich wie die Replizierereinrichtung kann auch die Verifizierungseinrichtung einen Server und ein Netzwerk aufweisen oder im Server eines Netzwerkes enthalten sein. Ferner ist es aber auch denkbar, die Verifizierungseinrichtung zentral bei der Zertifizierungsstelle und somit vorzugsweise in der zentralen Zertifikatstatusdatenbank oder alternativ verteilt in den lokalen Zertifikatstatusdatenbanken vorzusehen.

[0041] Eine gegenwärtig besonders bevorzugte Weiterbildung der zuvor genannten Ausführung der Erfindung zeichnet sich dadurch aus, daß die Verifizierungseinrichtung eine Verifizierungsanforderung einer lokalen Zertifikatstatusdatenbank an die zentrale Zertifikatstatusdatenbank übermittelt, dann von dieser an die betreffende lokale Zertifikatstatusdatenbank eine Verifizierungsantwort zurücksendet, die vorzugsweise einen Hashwert über Seriennummer, Fingerprint, Zertifikatstatus und/oder Daten des aktuellen Status enthält, und anhand dieser Verifizierungsantwort in der lokalen Zertifikatstatusdatenbank überprüft, ob deren Datenbestand mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank übereinstimmt. Anhand dieses Hashwertes kann auf Kundenseite bzw. auf seiten der betreffenden lokalen Zertifikatstatusdatenbank überprüft werden, ob der dortige Zertifikatstatusdatenbestand mit dem von der Zertifizierungsstelle verwalteten Original identisch ist, indem bei der Zertifizierungsstelle nur die für den betreffenden Kunden bzw. die betreffende lokale Zertifikatstatusdatenbank relevante Teil betrachtet wird.

[0042] Die zuvor erwähnte Verifizierungsanforderung, auch Verify-Request genannt, und die Verifizierungsantwort, auch Verify-Response genannt, bilden weitere Protokollelemente im zu übermittelnden Protokoll. Verifizierungsanforderungen können in regelmäßigen Abständen gestellt werden, um neben der Aktualität, die durch das zuvor erwähnte Ping-Request- und Ping-Response-Paar gewährleistet wird, die Integrität der lokalen Zertifikatstatusdatenbank des betreffenden Kunden nachweisbar zu halten.

[0043] Auch bei Fehlern im übermittelten Protokoll und/oder sonstigen verdächtigen Situationen, die auf einen möglichen Verlust der Integrität hinweisen, kann eine Verifizierungsanforderung gestellt werden.

[0044] Sollte bei der Verifizierung eine Unstimmigkeit aufgetreten sein – beispielsweise enthält die betreffende lo-

kale Zertifikatstatusdatenbank nicht diejenigen Daten, die sie gemäß der Zertifizierungsstelle enthalten sollte - und ist dies nicht lediglich durch einen Verlust von Update-Nachrichten begründet, so wird vom Kunden, also von seiten der betreffenden lokalen Zertifikatstatusdatenbank, eine komplette Neuerstellung des dortigen Datenbestandes veranlaßt. Für die komplette Neuerstellung sendet der Kunde bzw. dessen lokale Zertifikatstatusdatenbank eine Full-Update-Anforderung oder -Request an die Zertifizierungsstelle, die daraufhin den kompletten Datenbestand gemäß der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank durch eine spezielle Update-Nachricht überträgt.

[0045] Nachfolgend wird ein bevorzugtes Ausführungsbeispiel der Erfindung anhand der beiliegenden einzigen Figur näher erläutert, inder ein schematisches Blockschaltbild einer bevorzugten Ausführung eines Systems zur Statusabfrage von digitalen Zertifikaten dargestellt ist.

[0046] Hiernach ist bei einer Zertifizierungsstelle **2** eine zentrale Datenbank **4** installiert, in welcher sämtliche von der Zertifizierunginstanz **2** verwalteten Zertifikate und deren Status abgespeichert ist. Ein – vorzugsweises digitales – Zertifikat besteht aus Informationen über den Zertifikatsinhaber (z. B. Name, Ort, Land, Firma, Abteilung, Adresse etc.), den Namen des Zertifikatsausstellers, den Gültigkeitszeitraum und den Public Key sowie aus der Signatur der Zertifizierungsinstanz **2**.

[0047] Ferner weist die Zertifizierungsinstanz **2** einen Server **6** auf, der die zentrale Datenbank **4** mit einem Netzwerk **8** verbindet. Das Netzwerk **8** besteht üblicherweise aus reservierten Standleitungen, auf die Dritte keinen Zugriff haben. Aus Sicherheitsgründen sollte das Internet als Netzwerk dagegen nicht unbedingt genutzt werden.

[0048] Die Kunden der Zertifizierungsinstanz **2** sind über das Netzwerk **8** mit der Zertifizierungsinstanz **2** verbunden. Bei jedem Kunden ist mindestens ein Client **10** und eine daran angeschlossene lokale Datenbank **12** installiert.

[0049] In den lokalen Datenbanken **12** ist jeweils nur eine für den jeweiligen Kunden relevante Teilmenge des Datenbestandes der zentralen Datenbank **4** abgespeichert.

[0050] Mit Hilfe des Servers **6** werden über das Netzwerk **8**, ausgehend von der zentralen Datenbank **4**, die bei den Kunden installierten lokalen Datenbanken **12** aktualisiert. In den lokalen Datenbanken **12** wird jedoch nicht der komplette Datenbestand der zentralen Datenbank **4**, sondern nur der für den jeweiligen Kunden relevante Teil repliziert. Dabei wird die Änderung eines Zertifikatstatus oder die Neuausstellung von Zertifikaten initial in der zentralen Datenbank **4** der Zertifizierungsinstanz **2** vollzogen, und anschließend wird diese Änderung in die lokale Datenbank **12** des an dieser Änderung interessierten Kunden übertragen.

[0051] So wird ein bestimmtes Protokoll verwendet, mit dem, ausgehend von der zentralen Datenbank **4** bei der Zertifizierungsinstanz **2**, die für die einzelnen Kunden relevanten Zertifikatstatus mit den jeweiligen lokalen Datenbank **12** abgeglichen werden. Dieses Protokoll besteht im Einzelnen aus folgenden elementaren Nachrichten:

1. Update-Nachricht

[0052] Ein Protokollelement mit dem, ausgehend von der zentralen Datenbank **4**, die lokalen Datenbanken **12** aktualisiert werden, ist die Update-Nachricht. Eine Update-Nachricht ist mit einer Sequenznummer versehen und enthält Zertifikatinformationen wie z. B. Seriennummer, Fingerprint, Zertifikatstatus und Datum des aktuellen Status.

2. Ping-Request/Ping-Response

[0053] Um die Aktualität seiner lokalen Datenbank **12** zu verifizieren und den Empfang einer Update-Nachricht zu bestätigen, wird vom Client **10** des Kunden ein Ping-Request mit der Sequenznummer der zuletzt empfangenen Update-Nachricht an den Server **6** der Zertifizierungsinstanz **2** verschickt. Auf den Ping-Request antwortet der Server **6** der Zertifizierungsinstanz **2** mit einer Ping-Response, die die Sequenznummer der zuletzt übertragenen Update-Nachricht enthält und somit die Aktualität der Kundendatenbank bestätigt.

[0054] Weiterhin dient der Ping-Request dazu, "Denial-of-Service"-Attacken zu erkennen, wenn die entsprechende Ping-Response bzw. Update-Nachricht nicht innerhalb eines Timeouts zugestellt werden kann.

[0055] Das Protokollpaar, bestehend aus Ping-Request und Ping-Response, stellt den Normalfall dar und bildet die am häufigsten genutzten Protokollelemente, da die Bestätigung der Aktualität einer Datenbank wesentlich häufiger überprüft wird, als sich Änderungen und Neuausstellungen von Zertifikaten ergeben.

3. Verify-Request/Verify-Response

[0056] Die Protokollelemente Verify-Request und Verify-Response sind darauf ausgelegt, die Integrität aller Datenbanken **4** und **12** zu überprüfen, eine (lokale) Manipulation zu erkennen und ggf. den Neuaufbau einer Datenbank zu veranlassen.

[0057] Auf einen Verify-Request einer lokalen Datenbank **12** über den zugehörigen Client **10** erfolgt eine Verify-Response der Zertifizierungsinstanz **2** von der zentralen Datenbank **4** über den Server **6**, welcher einen Hash über die Seriennummer, den Fingerprint, den Zertifikatstatus und das Datum des aktuellen Status aller für den entsprechenden Kunden relevanten Zertifikate enthält. Anhand dieses Hash-Wertes kann dann auf Kundenseite überprüft werden, ob dessen gesamter Zertifikatsdatenbestand in der zugehörigen lokalen Datenbank **12** mit dem in der zentralen Datenbank **4** der Zertifizierungsinstanz **2** abgespeicherten und dort verwalteten Original identisch ist. Hierbei wird auch bei der Zertifizierungsinstanz **2** nur der für den jeweiligen Kunden relevante Teil betrachtet.

[0058] Verify-Requests können in regelmäßigen Abständen gestellt werden, um neben der Aktualität, die durch das Ping-Request und Ping-Response-Paar gewährleistet wird, auch die Integrität der lokalen Datenbanken **12** nachweisbar zu halten.

[0059] Auch bei Protokollfehlern und sonstigen verdächtigen Situationen, die auf einen möglichen Verlust der Integrität hinweisen, kann ein Verify-Request gestellt werden.

[0060] Sollte hierbei eine Unstimmigkeit aufgetreten sein, d. h. die lokale Datenbank **12** des jeweiligen Kunden nicht die Daten enthalten, die sie gemäß der Zertifizierungsinstanz **2** haben sollte, und liegt dies nicht am Verlust von Update-Nachrichten, so wird vom Kunden eine komplette Neuerstellung der zugehörigen lokalen Datenbank **12** initiiert.

4. Fullupdate-Request

[0061] Für die komplette Neuerstellung sendet der Kunde über seinen zugehörigen Client **10** einen Fullupdate-Request an den Server **6** der Zertifizierungsinstanz **2**, woraufhin der Server **6** den für diesen Kunden relevanten Teil des Datenbestandes aus der zentralen Datenbank **4** durch eine spezielle Update-Nachricht an die entsprechende lokale Datenbank **12** des Kunden überträgt.

Patentansprüche

1. System zur Statusabfrage von digitalen Zertifikaten, mit einer zentralen Zertifikatstatusdatenbank (**4**), **gekennzeichnet durch** eine Vielzahl von lokalen Zertifikatstatusdatenbanken (**12**), die von außen zugänglich sind und als Datenbestand jeweils nur eine Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (**4**) enthalten, und eine Repliziereinrichtung (**6**, **8**, **10**) zum Abgleich des Datenbestandes der lokalen Zertifikatstatusdatenbanken (**12**) jeweils mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (**4**).

2. System nach Anspruch 1, dadurch gekennzeichnet, daß die Repliziereinrichtung (**6**, **8**, **10**) den Datenbestand mindestens einer lokalen Zertifikatstatusdatenbank (**12**) in bestimmten, vorzugsweise gleichmäßigen, Zeitintervallen mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (**4**) wiederholt abgleicht.

3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Repliziereinrichtung (**6**, **8**, **10**), vorzugsweise regelmäßig, den Datenbestand der zentralen Zertifikatstatusdatenbank (**4**) auf Änderungen überprüft und nur dann den Datenbestand einer lokalen Zertifikatstatusdatenbank (**12**) aktualisiert, wenn sie in der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (**4**) Änderungen feststellt.

4. System nach mindestens einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Repliziereinrichtung einen Server (**6**) und ein Netzwerk (**8**) aufweist, über das die lokalen Zertifikatstatusdatenbanken (**12**) mit der zentralen Zertifikatstatusdatenbank (**4**) verbunden sind.

5. System nach Anspruch 4, dadurch gekennzeichnet, daß das Netzwerk (**8**) Änderungen einer Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (**4**) an die zugehörige lokale Zertifikatstatusdatenbank (**12**) überträgt.

6. System nach mindestens einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Repliziereinrichtung (**6**, **8**, **10**) von der zentralen Zertifikatstatusdatenbank (**4**) zu den lokalen Zertifikatstatusdatenbanken (**12**) Update-Nachrichten übermittelt, die mit einer Sequenznummer versehen sind und Zertifikationsinformationen, wie z. B. Seriennummer, Fingerprint, Zertifikatstatus und/oder Daten des aktuellen Status, enthalten.

7. System nach Anspruch 6, dadurch gekennzeichnet, daß die Repliziereinrichtung (**6**, **8**, **10**) in der betreffenden lokalen Zertifikatstatusdatenbank (**12**) die Sequenznummer der zuletzt empfangenen Update-Nachricht abfragt und mit der Sequenznummer der zuletzt an diese lokale Zertifikatstatusdatenbank (**12**) übertragenen Update-Nachricht in der zentralen Zertifikatstatusdatenbank (**4**) vergleicht und nur im Falle einer Übereinstimmung eine nächste Update-Nachricht von der zentralen Zertifikatstatusdatenbank (**4**) an die betreffende lokale Zertifikatstatusdatenbank (**12**) übermittelt.

8. System nach mindestens einem der Ansprüche 1 bis 7, gekennzeichnet durch eine Verifizierungseinrichtung (**6**, **8**, **10**) zur, vorzugsweise regelmäßigen, Überprüfung der Integrität der Datenbestände der lokalen Zertifikatstatusdatenbanken (**12**).

9. System nach Anspruch 8, dadurch gekennzeichnet, daß die Verifizierungseinrichtung (**6**, **8**, **10**) die Datenbestände der lokalen Zertifikatstatusdatenbanken (**12**) mit dem Datenbestand der zentralen Zertifikatstatusdatenbank (**4**) vergleicht.

10. System nach Anspruch 9, dadurch gekennzeichnet, daß die Verifizierungseinrichtung (**6**, **8**, **10**) eine Verifizierungsanforderung einer lokalen Zertifikatstatusdatenbank (**12**) an die zentrale Zertifikatstatusdatenbank (**4**) übermittelt, dann von dieser an die betreffende lokale Zertifikatstatusdatenbank (**12**) eine Verifizierungsanwort zurücksendet, die vorzugsweise einen Hashwert über Seriennummer, Fingerprint, Zertifikatstatus und/oder Daten des aktuellen Status enthält, und anhand dieser Verifizierungsantwort in der lokalen Zertifikatstatusdatenbank (**12**) überprüft, ob deren Datenbestand mit der entsprechenden Teilmenge des Datenbestandes der zentralen Zertifikatstatusdatenbank (**4**) übereinstimmt.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 100 61 102 A1
Int. Cl.[7]: G 06 F 17/30
Offenlegungstag: 27. Juni 2002